

United States District Court
Western District of New York

United States of America,

Plaintiff

vs

Joseph Bongiovanni

Defendant

**Defendant Joseph Bongiovanni's Objections
to Magistrate's Report, Recommendation & Order**

19-cr-227

Dated: September 9, 2022

James P. Harrington
HARRINGTON & MAHONEY
70 Niagara Street, 3rd Floor
Buffalo, NY 14202-3407
Ph: 716-853-3700
Facs: 716-853-3710
Attorneys for Defendant

Introduction

On August 5, 2022, the Hon. Michael J. Roemer, United States Magistrate Judge, filed a “Report, Recommendation and Order” (“R&R”) (Dkt 292) denying and granting in part certain motions of the defendant, Joseph Bongiovanni. One of the motions granted was a joinder to the motions of Mr. Bongiovanni’s co-defendant, Peter Gerace. Judge Roemer also issued a separate R&R for Mr. Gerace’s motions on August 5, 2022. (Dkt 291) To the extent those motions were denied and Mr. Gerace files objections, Mr. Bongiovanni joins in those objections.

The only issue in Judge Roemer’s Bongiovanni R&R that is objected to in this objection is Judge Roemer’s finding of good faith on the part of law enforcement in their search of Mr. Bongiovanni’s cell phone. Judge Roemer concluded that the Baltimore Washington International Airport (“BWI”) United States Customs and Border Protection (“CBP”) agents violated of Mr. Bongiovanni’s 4th Amendment search and seizure rights did not warrant suppression of seized information from his cell phone because the agents acted in “good faith.”

The R&R identifies the evolving case law regarding cell phone searches after *Riley v. California*, 573 U.S. 373 (2014),

“In the context of searches of electronic devices, including cell phones, the distinction between routine and nonroutine searches is an

area of evolving, and sometimes conflicting, jurisprudence. Moreover, neither the Supreme Court nor the Second Circuit have expressly ruled as to when the search of a cell phone at a border becomes nonroutine, and what is required by the Fourth Amendment when it does. Here, the Government urges that the search of Bongiovanni's cell phone on April 23, 2019 was a routine border search and therefore no warrant, probable cause or even reasonable suspicion was necessary.”

He analyzes the different terminology of border searches, i.e. basic v. forensic and routine v. non-routine in order to determine the type of search of Mr. Bongiovanni's phone and, if non-routine, whether it met the legal standard, reasonable suspicion, to make it impermissible.

In Mr. Bongiovanni's case, the agents attempted to do a forensic (advanced) search, where the use of the DOMEX machine would have been non-routine. When the machine failed to work, there was a “no harm no foul” situation at that point. The inquiry, however, did not end at the point. The R&R went on to discuss the following behavior of the agents. Their viewing, coupled with photographs taken of some of Mr. Bongiovanni's contact list and text messages, elevated the conduct to a non-routine search and seizure.

The R&R analyzes the information the agents were provided by Buffalo agents and found it wanting for reasonable suspicion. (Mr. Bongiovanni was returning from a family vacation in the Dominican Republic with his wife and stepson.)

The R&R found that the CBP agents search of Mr. Bongiovanni's cell phone on April

23, 2019, at the BWI airport was a non-routine (advanced) border search that required, but lacked, the reasonable suspicion of some type of criminal activity, border-related or otherwise. (R&R, p. 32).

The R&R also found that the search was a non-routine (advanced) because, even though the CBP agents manually searched the phone and did not connect it to the DOMEX machine, the CBP agents took the additional step of taking photos of the phone's contents including the contact list and numerous pages of text messages and saved them for later use in furtherance of criminal proceedings. None of the contents of the phone contained contraband or suggested criminal activity. This "stretched beyond what a traveler would expect to encounter at the border and constituted a significant intrusion upon defendant's privacy.". (R&R, p. 27). Had the officers simply manually clicked through some of the phone's contents and stopped when they did not find contraband or evidence, then the search would have been routine (aka basic). (R&R, p. 27).

Since the search was non-routine, the R&R found that a reasonable suspicion was required. (R&R, pp. 28-29). The CBP agents did not have the required reasonable suspicion of some type of criminal activity, border-related or otherwise because, even though reasonable suspicion is a low standard to meet, easier than probable cause, the Buffalo CBP and HSI agents (Mozg and Ryan) did not testify to knowing any specific and articulable facts about Bongiovanni's alleged criminal activity when they asked Baltimore CBP officers to conduct the search. "(T)he mere fact that agents were investigating Mr. Bongiovanni at the

time of search is insufficient to satisfy” the low bar that is reasonable suspicion. (R&R, pp. 29-30.)

The R&R, however, despite finding that the search of Mr. Bongiovanni’s phone violated his Fourth Amendment rights, determined that the officers had acted in good faith relying on binding appellate precedent and that the officers had testified that they had relied on longstanding CBP policy. (R&R, pp. 32-35). Binding appellate precedent means precedent from the 2nd Circuit and the Supreme Court. He reasoned that at the time of April 23, 2019, this was the state of the law:

1. The Supreme Court’s general rule was that *routine* (basic) border searches of persons and belongings did not require reasonable suspicion.
2. The 2nd Circuit did not clearly delineate *routine* (basic) from *non-routine* (advanced) searches of electronic devices.
3. Neither the Supreme Court nor the 2nd Circuit expressly require reasonable suspicion for conducting a non-routine border search of an electronic device.

(R&R, p. 33).

Mr. Bongiovanni agrees with the R&R that the search was non-routine and therefore

required a reasonable suspicion which the CBP officers did not have at the time of the search. He, however, disagrees with the R&R's application of the reliance-on-precedent good faith exception to the exclusionary rule that would normally be applied upon a finding of a Fourth Amendment violation. The R&R finds that on the reliance-on-precedent good faith exception which bars application of the exclusionary rule if a search is conducted in good faith if there is objectively reasonable reliance on binding precedent. (R&R, pp. 32-33).

Mr. Bongiovanni also agrees with the R&R that in April 2019 there were no Supreme Court cases *explicitly* stating what a non-routine border search was and the level of suspicion that would be required for a non-routine border search (*United States v. Montoya de Hernandez*, 473 U.S. 531 (1985); *United States v. Flores-Montano*, 541 U.S. 149 (2004) (“...we suggest no view on what level of suspicion, if any, is required for non-routine border searches”).

He further agrees with the R&R that in April 2019 the 2nd Circuit had not clearly delineated routine from non-routine border searches in regards to electronic devices. At that time, however, in April 2019, despite no explicit statement of when a search of an electronic device like a phone becomes non-routine, there was: (1) a general test to determine when a routine border search becomes a non-routine border search *and* (2) it had already been established that searching an electronic device was invasive of privacy.

United States v. Asbury, 586 F.2d 973, 975-976 (2d Cir. 1978), suggests that a border search becomes non-routine when a person's expectation of privacy is not reasonable (and

thus why a reasonable suspicion would be required to make those searches which involve extensive invasions of privacy reasonable) (finding that routine searches are made reasonable by the person's decision to cross the border since "...the person involved has no expectation of privacy that society is prepared to recognize as reasonable.") *United States v. Irving*, 452 F.3d 110 (2d Cir. 2006), seems to suggest that a non-routine border search is one which substantially infringes on a traveler's privacy rights. In *Irving*, the court looked at the intrusiveness of the search in distinguishing between routine and non-routine border searches, finding that "more invasive searches, like strip searches, require reasonable suspicion." Additionally, "*Levy* suggests that when officers not only search a traveler's possessions for contraband or obvious evidence of criminal activity, but also takes pictures and/or copy information to retain for use in a future criminal investigation or proceeding, a border search *may* become non routine." (R&R, p. 25 referencing *United States v. Levy*, 803 F.3d 120 (2d Cir. 2015).

Not only was there a general test in place at the time of the April 2019 search of Mr. Bongiovanni's phone that could have guided the officers to make a distinction between routine and non-routine searches, but the Supreme Court had already decided *Riley v. California*, 573 U.S. 373 (2014), which established that searching an electronic device would be highly invasive of privacy. *Riley* changed the landscape for everyone, including CPR agents. *Riley* found that cell phone searches are highly invasive of privacy since "cell phones differ in both a quantitative and qualitative sense from other objects" since they have "immense storage capacity" containing a person's "digital record of nearly every aspect of

their lives – from the mundane to the intimate.” In *Riley*, the Supreme Court found that “allowing the police to scrutinize such records (phone contents) on a routine basis is quite different from allowing them to search a personal item or two.” Though *Riley* concerned police arrests, this case recognized that phone searches are highly invasive of a person’s privacy.

Connecting the test to distinguish routine from non-routine searches and the recognition that phone searches implicate far more privacy concerns than searches of any other objects, the CBP agents and HSI agents officers requesting or conducting the search should have been aware that the search they conducted of the phone, taking photos of the contents for use in a future criminal proceeding, was highly intrusive of Mr. Bongiovanni’s privacy and therefore non-routine. It was clearly beyond any border security purposes.

The R&R’s heavy reliance on the judicial precedents to justify the good faith of the agents caused further research into the regulations controlling the agents’ conduct. Their belief that they were acting in accord with the regulations governing their conduct was misplaced. (It should be noted that the regulations were not offered into evidence, although the Court could take judicial notice of them, by either the government or Mr. Bongiovanni. This Court, however, as the court of primary jurisdiction, has the obligation to decide and consider arguments based on law and regulations. Alternatively, this issue could be remanded to Judge Roemer to consider this issue.)

The CBP regulation, *CBP Direction 3340-049A on Border Search of Electronic*

Devices Containing Information (Exhibit A), which had been in place since January 2018, post *Riley* and a whole year before the border search of Mr. Bongiovanni's phone at BWI Airport – replaced Direction 3340-049 which had been in effect since August of 2009. The 2018 updated CBP policy changed the old policy by explicitly defining advanced (non-routine) and basic (routine) searches of electronic devices and by explicitly requiring reasonable suspicion for advanced (non-routine) searches.

The Advanced Search regulation states “In instances in which there is reasonable suspicion of activity in violation of the laws enforced or administered by CBP. . .” an advanced search may be conducted. Based on this regulation, with the finding in the R&R that there is no reasonable suspicion in Mr. Bongiovanni's case, there can be no good faith exception. The fact that there is a lack of certainty in case law does not affect the stated regulation. The good faith exception should not have been applied in this case.

Also the agents essentially believed they were doing a basic search because of the following three reasons: (1) Agent Carter testified that an advanced search requires a connection with a DOMEX machine that will extract information from the phone and the officers conducted a manual search of the phone. (2) Agent Carter testified that an advanced search could take several hours and produce much more data than a basic search could. (Transcript p. 21. 109-110) while a basic search could last about 15-30 minutes. He further testified that the CBP had Mr. Bongiovanni's phone for about 15-20 minutes and only produced 14 pages of photos. (Transcript p. 20-21, 43, 45, 71). Finally, (3) Agent Carter

also testified that during a basic search, if there is information that they are taking from the phone, that they need to review later, they would use government phones to take pictures of the content. It should be noted that the 2018 CBP Policy (Directive 3340-049A) states that the purpose of the advanced search is to not just gain access to the device, but to review, copy, and/or analyze its contents, while the definition of the basic search only allows for an Officer to examine an electronic device and review and analyze information encountered at the border (CBP Directive 3340-049A p. 4, Sections 4.1.3-5.1.4). The CBP's definition of a basic search does not mention anything about retaining information. *Id.* Therefore, though the advanced search definition states that the phone must be connected to external equipment, the purpose of the advanced search is broader than that of the basic search. Despite not having connected the phone to the DOMEX machine (because it did not work), arguably the copying and retention of the information should have signaled to the officers that they were moving beyond the scope of a basic search as the R&R states. Arguably, the extraction of information from a device and not the mechanics of how that information is extracted should be a consideration in determining whether or not a search is basic or advanced.

Conclusion

For the reasons stated, the Court should grant Mr. Bongiovanni's challenge to the R&R's finding of a good faith exception to his 4th Amendment search and seizure or, in the

alternative remand the case to Judge Roemer for his reconsideration of that issue in light of the argument above regarding the CPB regulations.

Dated: September 9, 2022

Respectfully submitted,
/s/ James P. Harrington

James P. Harrington
HARRINGTON & MAHONEY
70 Niagara Street, 3rd Floor
Buffalo, NY 14202-3093
(716) 853-3700 (*voice*)
(716) 853-3710 (*facsimile*)
jph@harringtonmahoney.com

EXHIBIT A

U.S. CUSTOMS AND BORDER PROTECTION

CBP DIRECTIVE NO. 3340-049A

DATE: January 4, 2018

ORIGINATING OFFICE: FO:TO

SUPERSEDES: Directive 3340-049

REVIEW DATE: January 2021

SUBJECT: BORDER SEARCH OF ELECTRONIC DEVICES

1 PURPOSE. To provide guidance and standard operating procedures for searching, reviewing, retaining, and sharing information contained in computers, tablets, removable media, disks, drives, tapes, mobile phones, cameras, music and other media players, and any other communication, electronic, or digital devices subject to inbound and outbound border searches by U.S. Customs and Border Protection (CBP). These searches are conducted in furtherance of CBP's customs, immigration, law enforcement, and homeland security responsibilities and to ensure compliance with customs, immigration, and other laws that CBP is authorized to enforce and administer.

These searches are part of CBP's longstanding practice and are essential to enforcing the law at the U.S. border and to protecting border security. They help detect evidence relating to terrorism and other national security matters, human and bulk cash smuggling, contraband, and child pornography. They can also reveal information about financial and commercial crimes, such as those relating to copyright, trademark, and export control violations. They can be vital to risk assessments that otherwise may be predicated on limited or no advance information about a given traveler or item, and they can enhance critical information sharing with, and feedback from, elements of the federal government responsible for analyzing terrorist threat information. Finally, searches at the border are often integral to a determination of an individual's intentions upon entry and provide additional information relevant to admissibility under the immigration laws.

2 POLICY

2.1 CBP will protect the rights of individuals against unreasonable search and seizure and ensure privacy protections while accomplishing its enforcement mission.

2.2 All CBP Officers, Border Patrol Agents, Air and Marine Agents, Office of Professional Responsibility Agents, and other officials authorized by CBP to perform border searches shall adhere to the policy described in this Directive and any implementing policy memoranda or musters.

- 2 -

2.3 This Directive governs border searches of electronic devices – including any inbound or outbound search pursuant to longstanding border search authority and conducted at the physical border, the functional equivalent of the border, or the extended border, consistent with law and agency policy. For purposes of this Directive, this excludes actions taken to determine if a device functions (e.g., turning a device on and off); or actions taken to determine if physical contraband is concealed within the device itself; or the review of information voluntarily provided by an individual in an electronic format (e.g., when an individual shows an e-ticket on an electronic device to an Officer, or when an alien proffers information to establish admissibility). This Directive does not limit CBP's authority to conduct other lawful searches of electronic devices, such as those performed pursuant to a warrant, consent, or abandonment, or in response to exigent circumstances; it does not limit CBP's ability to record impressions relating to border encounters; it does not restrict the dissemination of information as required by applicable statutes and Executive Orders.

2.4 This Directive does not govern searches of shipments containing commercial quantities of electronic devices (e.g., an importation of hundreds of laptop computers transiting from the factory to the distributor).

2.5 This Directive does not supersede *Restrictions on Importation of Seditious Matter*, Directive 2210-001A. Seditious materials encountered through a border search should continue to be handled pursuant to Directive 2210-001A or any successor thereto.

2.6 This Directive does not supersede *Processing Foreign Diplomatic and Consular Officials*, Directive 3340-032. Diplomatic and consular officials encountered at the border, the functional equivalent of the border (FEB), or extended border should continue to be processed pursuant to Directive 3340-032 or any successor thereto.

2.7 This Directive applies to searches performed by or at the request of CBP. With respect to searches performed by U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) Special Agents exercise concurrently-held border search authority that is covered by ICE's own policy and procedures. When CBP detains, seizes, or retains electronic devices, or copies of information therefrom, and conveys such to ICE for analysis, investigation, and disposition (with appropriate documentation), the conveyance to ICE is not limited by the terms of this Directive, and ICE policy will apply upon receipt by ICE.

3 DEFINITIONS

3.1 Officer. A Customs and Border Protection Officer, Border Patrol Agent, Air and Marine Agent, Office of Professional Responsibility Special Agent, or any other official of CBP authorized to conduct border searches.

3.2 Electronic Device. Any device that may contain information in an electronic or digital form, such as computers, tablets, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players.

3.3 **Destruction.** For electronic records, destruction is deleting, overwriting, or degaussing in compliance with CBP Information Systems Security Policies and Procedures Handbook, CIS HB 1400-05C.

4 AUTHORITY/REFERENCES. 6 U.S.C. §§ 122, 202, 211; 8 U.S.C. §§ 1225, 1357, and other pertinent provisions of the immigration laws and regulations; 19 U.S.C. §§ 482, 507, 1461, 1496, 1581, 1582, 1589a, 1595a(d), and other pertinent provisions of customs laws and regulations; 31 U.S.C. § 5317 and other pertinent provisions relating to monetary instruments; 22 U.S.C. § 401 and other laws relating to exports; Guidelines for Detention and Seizures of Pornographic Materials, Directive 4410-001B; Disclosure of Business Confidential Information to Third Parties, Directive 1450-015; Accountability and Control of Custody Receipt for Detained and Seized Property (CF6051), Directive 5240-005.

The plenary authority of the Federal Government to conduct searches and inspections of persons and merchandise crossing our nation's borders is well-established and extensive; control of the border is a fundamental principle of sovereignty. "[T]he United States, as sovereign, has the inherent authority to protect, and a paramount interest in protecting, its territorial integrity." *United States v. Flores-Montano*, 541 U.S. 149, 153 (2004). "The Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border. Time and again, [the Supreme Court has] stated that 'searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border.'" *Id.* at 152-53 (quoting *United States v. Ramsey*, 431 U.S. 606, 616 (1977)). "Routine searches of the persons and effects of entrants [into the United States] are not subject to any requirement of reasonable suspicion, probable cause, or warrant." *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985). Additionally, the authority to conduct border searches extends not only to persons and merchandise entering the United States, but applies equally to those departing the country. *See, e.g., United States v. Boumelhem*, 339 F.3d 414, 422-23 (6th Cir. 2003); *United States v. Odutayo*, 406 F.3d 386, 391-92 (5th Cir. 2005); *United States v. Oriakhi*, 57 F.3d 1290, 1296-97 (4th Cir. 1995); *United States v. Ezeiruaku*, 936 F.2d 136, 143 (3d Cir. 1991); *United States v. Cardona*, 769 F.2d 625, 629 (9th Cir. 1985); *United States v. Udofot*, 711 F.2d 831, 839-40 (8th Cir. 1983).

As a constitutional matter, border search authority is premised in part on a reduced expectation of privacy associated with international travel. *See Flores-Montano*, 541 U.S. at 154 (noting that "the expectation of privacy is less at the border than it is in the interior"). Persons and merchandise encountered by CBP at the international border are not only subject to inspection under U.S. law, they also have been or will be abroad and generally subject to the legal authorities of at least one other sovereign. *See Boumelhem*, 339 F.3d at 423.

In addition to longstanding federal court precedent recognizing the constitutional authority of the U.S. government to conduct border searches, numerous federal statutes and regulations also authorize CBP to inspect and examine all individuals and merchandise entering or departing the United States, including all types of personal property, such as electronic devices. *See, e.g.,* 8 U.S.C. §§ 1225, 1357; 19 U.S.C. §§ 482, 507, 1461, 1496, 1581, 1582, 1589a, 1595a; *see also* 19 C.F.R. § 162.6 ("All persons, baggage, and merchandise arriving in the Customs territory of

the United States from places outside thereof are liable to inspection and search by a Customs officer.”). These authorities support CBP’s enforcement and administration of federal law at the border and facilitate the inspection of merchandise and people to fulfill the immigration, customs, agriculture, and counterterrorism missions of the Department. This includes, among other things, the responsibility to “ensure the interdiction of persons and goods illegally entering or exiting the United States”; “detect, respond to, and interdict terrorists, drug smugglers and traffickers, human smugglers and traffickers, and other persons who may undermine the security of the United States”; “safeguard the borders of the United States to protect against the entry of dangerous goods”; “enforce and administer all immigration laws”; “deter and prevent the illegal entry of terrorists, terrorist weapons, persons, and contraband”; and “conduct inspections at [] ports of entry to safeguard the United States from terrorism and illegal entry of persons.” 6 U.S.C. § 211.

CBP must conduct border searches of electronic devices in accordance with statutory and regulatory authorities and applicable judicial precedent. CBP’s broad authority to conduct border searches is well-established, and courts have rejected a categorical exception to the border search doctrine for electronic devices. Nevertheless, as a policy matter, this Directive imposes certain requirements, above and beyond prevailing constitutional and legal requirements, to ensure that the authority for border search of electronic devices is exercised judiciously, responsibly, and consistent with the public trust.

5 PROCEDURES

5.1 Border Searches

5.1.1 Border searches may be performed by an Officer or other individual authorized to perform or assist in such searches (e.g., under 19 U.S.C. § 507).

5.1.2 Border searches of electronic devices may include searches of the information stored on the device when it is presented for inspection or during its detention by CBP for an inbound or outbound border inspection. The border search will include an examination of only the information that is resident upon the device and accessible through the device’s operating system or through other software, tools, or applications. Officers may not intentionally use the device to access information that is solely stored remotely. To avoid retrieving or accessing information stored remotely and not otherwise present on the device, Officers will either request that the traveler disable connectivity to any network (e.g., by placing the device in airplane mode), or, where warranted by national security, law enforcement, officer safety, or other operational considerations, Officers will themselves disable network connectivity. Officers should also take care to ensure, throughout the course of a border search, that they do not take actions that would make any changes to the contents of the device.

5.1.3 Basic Search. Any border search of an electronic device that is not an advanced search, as described below, may be referred to as a basic search. In the course of a basic search, with or without suspicion, an Officer may examine an electronic device and may review and analyze information encountered at the border, subject to the requirements and limitations provided herein and applicable law.

5.1.4 Advanced Search. An advanced search is any search in which an Officer connects external equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents. In instances in which there is reasonable suspicion of activity in violation of the laws enforced or administered by CBP, or in which there is a national security concern, and with supervisory approval at the Grade 14 level or higher (or a manager with comparable responsibilities), an Officer may perform an advanced search of an electronic device. Many factors may create reasonable suspicion or constitute a national security concern; examples include the existence of a relevant national security-related lookout in combination with other articulable factors as appropriate, or the presence of an individual on a government-operated and government-vetted terrorist watch list.

5.1.5 Searches of electronic devices will be documented in appropriate CBP systems, and advanced searches should be conducted in the presence of a supervisor. In circumstances where operational considerations prevent a supervisor from remaining present for the entire advanced search, or where supervisory presence is not practicable, the examining Officer shall, as soon as possible, notify the appropriate supervisor about the search and any results thereof.

5.1.6 Searches of electronic devices should be conducted in the presence of the individual whose information is being examined unless there are national security, law enforcement, officer safety, or other operational considerations that make it inappropriate to permit the individual to remain present. Permitting an individual to remain present during a search does not necessarily mean that the individual shall observe the search itself. If permitting an individual to observe the search could reveal law enforcement techniques or potentially compromise other operational considerations, the individual will not be permitted to observe the search itself.

5.2 Review and Handling of Privileged or Other Sensitive Material

5.2.1 Officers encountering information they identify as, or that is asserted to be, protected by the attorney-client privilege or attorney work product doctrine shall adhere to the following procedures.

5.2.1.1 The Officer shall seek clarification, if practicable in writing, from the individual asserting this privilege as to specific files, file types, folders, categories of files, attorney or client names, email addresses, phone numbers, or other particulars that may assist CBP in identifying privileged information.

5.2.1.2 Prior to any border search of files or other materials over which a privilege has been asserted, the Officer will contact the CBP Associate/Assistant Chief Counsel office. In coordination with the CBP Associate/Assistant Chief Counsel office, which will coordinate with the U.S. Attorney's Office as needed, Officers will ensure the segregation of any privileged material from other information examined during a border search to ensure that any privileged material is handled appropriately while also ensuring that CBP accomplishes its critical border security mission. This segregation process will occur through the establishment and employment of a Filter Team composed of legal and operational representatives, or through another appropriate measure with written concurrence of the CBP Associate/Assistant Chief Counsel office.

5.2.1.3 At the completion of the CBP review, unless any materials are identified that indicate an imminent threat to homeland security, copies of materials maintained by CBP and determined to be privileged will be destroyed, except for any copy maintained in coordination with the CBP Associate/Assistant Chief Counsel office solely for purposes of complying with a litigation hold or other requirement of law.

5.2.2 Other possibly sensitive information, such as medical records and work-related information carried by journalists, shall be handled in accordance with any applicable federal law and CBP policy. Questions regarding the review of these materials shall be directed to the CBP Associate/Assistant Chief Counsel office, and this consultation shall be noted in appropriate CBP systems.

5.2.3 Officers encountering business or commercial information in electronic devices shall treat such information as business confidential information and shall protect that information from unauthorized disclosure. Depending on the nature of the information presented, the Trade Secrets Act, the Privacy Act, and other laws, as well as CBP policies, may govern or restrict the handling of the information. Any questions regarding the handling of business or commercial information may be directed to the CBP Associate/Assistant Chief Counsel office or the CBP Privacy Officer, as appropriate.

5.2.4 Information that is determined to be protected by law as privileged or sensitive will only be shared with agencies or entities that have mechanisms in place to protect appropriately such information, and such information will only be shared in accordance with this Directive.

5.3 Review and Handling of Passcode-Protected or Encrypted Information

5.3.1 Travelers are obligated to present electronic devices and the information contained therein in a condition that allows inspection of the device and its contents. If presented with an electronic device containing information that is protected by a passcode or encryption or other security mechanism, an Officer may request the individual's assistance in presenting the electronic device and the information contained therein in a condition that allows inspection of the device and its contents. Passcodes or other means of access may be requested and retained as needed to facilitate the examination of an electronic device or information contained on an electronic device, including information on the device that is accessible through software applications present on the device that is being inspected or has been detained, seized, or retained in accordance with this Directive.

5.3.2 Passcodes and other means of access obtained during the course of a border inspection will only be utilized to facilitate the inspection of devices and information subject to border search, will be deleted or destroyed when no longer needed to facilitate the search of a given device, and may not be utilized to access information that is only stored remotely.

5.3.3 If an Officer is unable to complete an inspection of an electronic device because it is protected by a passcode or encryption, the Officer may, in accordance with section 5.4 below, detain the device pending a determination as to its admissibility, exclusion, or other disposition.

5.3.4 Nothing in this Directive limits CBP's ability, with respect to any device presented in a manner that is not readily accessible for inspection, to seek technical assistance, or to use external equipment or take other reasonable measures, or in consultation with the CBP Associate/Assistant Chief Counsel office to pursue available legal remedies, to render a device in a condition that allows for inspection of the device and its contents.

5.4 Detention and Review in Continuation of Border Search of Information

5.4.1 Detention and Review by CBP

An Officer may detain electronic devices, or copies of information contained therein, for a brief, reasonable period of time to perform a thorough border search. The search may take place on-site or at an off-site location, and is to be completed as expeditiously as possible. Unless extenuating circumstances exist, the detention of devices ordinarily should not exceed five (5) days. Devices must be presented in a manner that allows CBP to inspect their contents. Any device not presented in such a manner may be subject to exclusion, detention, seizure, or other appropriate action or disposition.

5.4.1.1 Approval of and Time Frames for Detention. Supervisory approval is required for detaining electronic devices, or copies of information contained therein, for continuation of a border search after an individual's departure from the port or other location of detention. Port Director; Patrol Agent in Charge; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or other equivalent level manager approval is required to extend any such detention beyond five (5) days. Extensions of detentions exceeding fifteen (15) days must be approved by the Director, Field Operations; Chief Patrol Agent; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or other equivalent manager, and may be approved and re-approved in increments of no more than seven (7) days. Approvals for detention and any extension thereof shall be noted in appropriate CBP systems.

5.4.1.2 Destruction. Except as noted in section 5.5 or elsewhere in this Directive, if after reviewing the information pursuant to the time frames discussed in section 5.4, there is no probable cause to seize the device or the information contained therein, any copies of the information held by CBP must be destroyed, and any electronic device must be returned. Upon this determination, the copy of the information will be destroyed as expeditiously as possible, but no later than seven (7) days after such determination unless circumstances require additional time, which must be approved by a supervisor and documented in an appropriate CBP system and which must be no later than twenty-one (21) days after such determination. The destruction shall be noted in appropriate CBP systems.

5.4.1.3 Notification of Border Search. When a border search of information is conducted on an electronic device, the individual subject to search will be notified of the purpose and authority for such search, how the individual may obtain more information on reporting concerns about their search, and how the individual may seek redress from the agency if he or she feels aggrieved by a search. If the Officer or other appropriate CBP official determines that the fact of conducting this search cannot be disclosed to the individual transporting the device without

impairing national security, law enforcement, officer safety, or other operational interests, notification may be withheld.

5.4.1.4 Custody Receipt. If CBP determines it is necessary to detain temporarily an electronic device to continue the search, the Officer detaining the device shall issue a completed Form 6051D to the individual prior to the individual's departure.

5.4.2 Assistance

Officers may request assistance that may be needed to access and search an electronic device and the information stored therein. Except with respect to assistance sought within CBP or from ICE, the following subsections of 5.4.2 govern requests for assistance.

5.4.2.1 Technical Assistance. Officers may sometimes need technical assistance to render a device and its contents in a condition that allows for inspection. For example, Officers may encounter a device or information that is not readily accessible for inspection due to encryption or password protection. Officers may also require translation assistance to inspect information that is in a foreign language. In such situations, Officers may convey electronic devices or copies of information contained therein to seek technical assistance.

5.4.2.2 Subject Matter Assistance – With Reasonable Suspicion or National Security Concern. Officers may encounter information that requires referral to subject matter experts to determine the meaning, context, or value of information contained therein as it relates to the laws enforced or administered by CBP. Therefore, Officers may convey electronic devices or copies of information contained therein for the purpose of obtaining subject matter assistance when there is a national security concern or they have reasonable suspicion of activities in violation of the laws enforced or administered by CBP.

5.4.2.3 Approvals for Seeking Assistance. Requests for assistance require supervisory approval and shall be properly documented and recorded in CBP systems. If an electronic device is to be detained after the individual's departure, the Officer detaining the device shall execute a Form 6051D and provide a copy to the individual prior to the individual's departure. All transfers of the custody of the electronic device will be recorded on the Form 6051D.

5.4.2.4 Electronic devices should be transferred only when necessary to render the requested assistance. Otherwise, a copy of data from the device should be conveyed in lieu of the device in accordance with this Directive.

5.4.2.5 When an electronic device or information contained therein is conveyed for assistance, the individual subject to search will be notified of the conveyance unless the Officer or other appropriate CBP official determines, in consultation with the receiving agency or other entity as appropriate, that notification would impair national security, law enforcement, officer safety, or other operational interests. If CBP seeks assistance for counterterrorism purposes, if a relevant national security-related lookout applies, or if the individual is on a government-operated and government-vetted terrorist watch list, the individual will not be notified of the conveyance, the existence of a relevant national security-related lookout, or his or her presence on a watch list.

When notification is made to the individual, the Officer will annotate the notification in CBP systems and on the Form 6051D.

5.4.3 Responses and Time for Assistance

5.4.3.1 Responses Required. Agencies or entities receiving a request for assistance in conducting a border search are expected to provide such assistance as expeditiously as possible. Where subject matter assistance is requested, responses should include all appropriate findings, observations, and conclusions relating to the laws enforced or administered by CBP.

5.4.3.2 Time for Assistance. Responses from assisting agencies or entities are expected in an expeditious manner so that CBP may complete the border search in a reasonable period of time. Unless otherwise approved by the Director Field Operations; Chief Patrol Agent; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or equivalent level manager, responses should be received within fifteen (15) days. If the assisting agency or entity is unable to respond in that period of time, the Director Field Operations; Chief Patrol Agent; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or equivalent level manager may permit extensions in increments of seven (7) days.

5.4.3.3 Revocation of a Request for Assistance. If at any time a CBP supervisor involved in a request for assistance is not satisfied with the assistance provided, the timeliness of assistance, or any other articulable reason, the request for assistance may be revoked, and the CBP supervisor may require the assisting agency or entity to return to CBP all electronic devices provided, and any copies thereof, as expeditiously as possible, except as noted in 5.5.2.3. Any such revocation shall be documented in appropriate CBP systems. When CBP has revoked a request for assistance because of the lack of a timely response, CBP may initiate the request with another agency or entity pursuant to the procedures outlined in this Directive.

5.4.3.4 Destruction. Except as noted in section 5.5.1 below or elsewhere in this Directive, if after reviewing information, probable cause to seize the device or the information from the device does not exist, CBP will retain no copies of the information.

5.5 Retention and Sharing of Information Found in Border Searches

5.5.1 Retention and Sharing of Information Found in Border Searches

5.5.1.1 Retention with Probable Cause. Officers may seize and retain an electronic device, or copies of information from the device, when, based on a review of the electronic device encountered or on other facts and circumstances, they determine there is probable cause to believe that the device, or copy of the contents from the device, contains evidence of a violation of law that CBP is authorized to enforce or administer.

5.5.1.2 Retention of Information in CBP Privacy Act-Compliant Systems. Without probable cause to seize an electronic device or a copy of information contained therein, CBP may retain only information relating to immigration, customs, and other enforcement matters if such retention is consistent with the applicable system of records notice. For example, information

collected in the course of immigration processing for the purposes of present and future admissibility of an alien may be retained in the A-file, Central Index System, TECS, and/or E3 or other systems as may be appropriate and consistent with the policies governing such systems.

5.5.1.3 Sharing Generally. Nothing in this Directive limits the authority of CBP to share copies of information contained in electronic devices (or portions thereof), which are retained in accordance with this Directive, with federal, state, local, and foreign law enforcement agencies to the extent consistent with applicable law and policy.

5.5.1.4 Sharing of Terrorism Information. Nothing in this Directive is intended to limit the sharing of terrorism-related information to the extent the sharing of such information is authorized by statute, Presidential Directive, or DHS policy. Consistent with 6 U.S.C. § 122(d)(2) and other applicable law and policy, CBP, as a component of DHS, will promptly share any terrorism information encountered in the course of a border search with entities of the federal government responsible for analyzing terrorist threat information. In the case of such terrorism information sharing, the entity receiving the information will be responsible for providing CBP with all appropriate findings, observations, and conclusions relating to the laws enforced by CBP. The receiving entity will be responsible for managing retention and disposition of information it receives in accordance with its own legal authorities and responsibilities.

5.5.1.5 Safeguarding Data During Storage and Conveyance. CBP will appropriately safeguard information retained, copied, or seized under this Directive and during conveyance. Appropriate safeguards include keeping materials in locked cabinets or rooms, documenting and tracking copies to ensure appropriate disposition, and other safeguards during conveyance such as password protection or physical protections. Any suspected loss or compromise of information that contains personal data retained, copied, or seized under this Directive must be immediately reported to the CBP Office of Professional Responsibility and to the Port Director; Patrol Agent in Charge; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or equivalent level manager.

5.5.1.6 Destruction. Except as noted in this section or elsewhere in this Directive, if after reviewing information, there exists no probable cause to seize the information, CBP will retain no copies of the information.

5.5.2 Retention by Agencies or Entities Providing Technical or Subject Matter Assistance

5.5.2.1 During Assistance. All electronic devices, or copies of information contained therein, provided to an assisting agency or entity may be retained for the period of time needed to provide the requested assistance to CBP or in accordance with section 5.5.2.3 below.

5.5.2.2 Return or Destruction. CBP will request that at the conclusion of the requested assistance, all information be returned to CBP as expeditiously as possible, and that the assisting agency or entity advise CBP in accordance with section 5.4.3 above. In addition, the assisting agency or entity should destroy all copies of the information conveyed unless section 5.5.2.3 below applies. In the event that any electronic devices are conveyed, they must not be destroyed;

they are to be returned to CBP unless seized by an assisting agency based on probable cause or retained per 5.5.2.3.

5.5.2.3 Retention with Independent Authority. If an assisting federal agency elects to continue to retain or seize an electronic device or information contained therein, that agency assumes responsibility for processing the retention or seizure. Copies may be retained by an assisting federal agency only if and to the extent that it has the independent legal authority to do so – for example, when the information relates to terrorism or national security and the assisting agency is authorized by law to receive and analyze such information. In such cases, the retaining agency should advise CBP of its decision to retain information under its own authority.

5.6 Reporting Requirements

5.6.1 The Officer performing the border search of information shall be responsible for completing all after-action reporting requirements. This responsibility includes ensuring the completion of all applicable documentation such as the Form 6051D when appropriate, and creation and/or updating records in CBP systems. Reports are to be created and updated in an accurate, thorough, and timely manner. Reports must include all information related to the search through the final disposition including supervisory approvals and extensions when appropriate.

5.6.2 In instances where an electronic device or copy of information contained therein is forwarded within CBP as noted in section 5.4.1, the receiving Officer is responsible for recording all information related to the search from the point of receipt forward through the final disposition.

5.6.3 Reporting requirements for this Directive are in addition to, and do not replace, any other applicable reporting requirements.

5.7 Management Requirements

5.7.1 The duty supervisor shall ensure that the Officer completes a thorough inspection and that all notification, documentation, and reporting requirements are accomplished.

5.7.2 The appropriate CBP second-line supervisor shall approve and monitor the status of the detention of all electronic devices or copies of information contained therein.

5.7.3 The appropriate CBP second-line supervisor shall approve and monitor the status of the transfer of any electronic device or copies of information contained therein for translation, decryption, or subject matter assistance from another agency or entity.

5.7.4 The Director, Field Operations; Chief Patrol Agent; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or equivalent level manager shall establish protocols to monitor the proper documentation and recording of searches conducted pursuant to this Directive and the detention, transfer, and final disposition of electronic devices or copies of

information contained therein in order to ensure compliance with the procedures outlined in this Directive.

5.7.5 Officers will ensure, in coordination with field management as appropriate, that upon receipt of any subpoena or other request for testimony or information regarding the border search of an electronic device in any litigation or proceeding, notification is made to the appropriate CBP Associate/Assistant Chief Counsel office.

6 MEASUREMENT. CBP Headquarters will continue to develop and maintain appropriate mechanisms to ensure that statistics regarding border searches of electronic devices, and the results thereof, can be generated from CBP systems using data elements entered by Officers pursuant to this Directive.

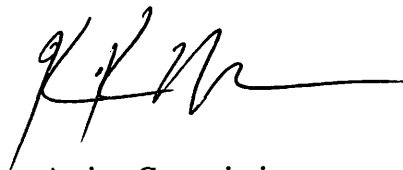
7 AUDIT. CBP Management Inspection will develop and periodically administer an auditing mechanism to review whether border searches of electronic devices are being conducted in conformity with this Directive.

8 NO PRIVATE RIGHT CREATED. This Directive is an internal policy statement of U.S. Customs and Border Protection and does not create or confer any rights, privileges, or benefits on any person or party.

9 REVIEW. This Directive shall be reviewed and updated, as necessary, at least every three years.

10 DISCLOSURE. This Directive may be shared with the public.

11 SUPERSEDES. Procedures for Border Search/Examination of Documents, Paper, and Electronic Information (July 5, 2007) and Policy Regarding Border Search of Information (July 16, 2008), to the extent they pertain to electronic devices; CBP Directive No. 3340-049, Border Searches of Electronic Devices Containing Information (August 20, 2009).

A handwritten signature in black ink, appearing to be 'K. J. M.', followed by a long horizontal line extending to the right.

Acting Commissioner